FORM PTO-1390 (REV. 11-2000) U S DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE **TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371**	ATTORNEY 'S DOCKET NUMBER PTT-124 (402562US) U S APPLICATION NO (If known, see 37 CFR 1 5 09/937415

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/EP00/02617	23 March 2000	01 April 1999

TITLE OF INVENTION METHOD FOR ENCIPHERING A SERIES OF SYMBOLS APPLYING A FUNCTION AND A KEY

APPLICANT(S) FOR DO/EO/US
MULLER, Frank; PINS, Sharon Christie Lesley; ROELOFSEN, Gerrit

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. □ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. □ This is an express request to begin national examination procedures (35 U.S.C. 371(f)). The submission must include items (5), (6), (9) and (21) indicated below.
4. □ The US has been elected by the expiration of 19 months from the priority date (Article 31).
5. □ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. □ is attached hereto (required only if not communicated by the International Bureau).
   b. □ has been communicated by the International Bureau.
   c. □ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. □ An English language translation of the International Application as filed (35 U.S.C. 371(c)(2)).
   a. □ is attached hereto.
   b. □ has been previously submitted under 35 U.S.C. 154(d)(4).
7. □ Amendments to the claims of the International Aplication under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. □ are attached hereto (required only if not communicated by the International Bureau).
   b. □ have been communicated by the International Bureau.
   c. □ have not been made; however, the time limit for making such amendments has NOT expired.
   d. □ have not been made and will not be made.
8. □ An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371 (c)(3)).
9. □ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. □ An English lanugage translation of the annexes of the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11 to 20 below concern document(s) or information included:

11. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98. (with modified Form PTO/SB/08A/B, copy of International Search Report and six (6) cited references)
12. □ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☒ A FIRST preliminary amendment. (with 2 pps. of substitute/clean claims)
14. □ A SECOND or SUBSEQUENT preliminary amendment.
15. □ A substitute specification.
16. □ A change of power of attorney and/or address letter.
17. □ A computer-readable form of the sequence listing in accordance with PCT Rule 13ter.2 and 35 U.S.C. 1.821 - 1.825.
18. □ A second copy of the published international application under 35 U.S.C. 154(d)(4).
19. □ A second copy of the English language translation of the international application under 35 U.S.C. 154(d)(4).
20. ☒ Other items or information: postcard receipt, Cover Letter (2 pps.), copy of International Publication No. WO 00/60807 with Three (3) sheets of formal drawings (FIGs. 1-4), copy of Request (7 pps.), copy of Notification of International Application Number and of International Filing Date (1 pps.), copy of PCT Demand (6 pps.), copy of Notification of Transmittal of International Preliminary Examination Report and International Examination Report, with amended sheets (16 pps.), Submission of Priority Document with Certified copy (with English translation) of Netherlands Number 1011719.

U.S. APPLICATION NO (if known, see 37 CFR 1.5)	INTERNATIONAL APPLICATION NO	ATTORNEY'S DOCKET NUMBER
09/937415	PCT/EP00/02617	PTT-124(402562US)

	CALCULATIONS	PTO USE ONLY
21. ☒ The following fees are submitted: **BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)):** Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO .... **$1000.00** International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO .... **$860.00** International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO .... **$710.00** International preliminary examination fee (37 CFR 1.482) paid to USPTO but all claims did not satisfy provisions of PCT Article 33(1)-(4) .... **$690.00** International preliminary examination fee (37 CFR 1.482) paid to USPTO and all claims satisfied provisions of PCT Article 33(1)-(4) **$100.00**		
ENTER APPROPRIATE BASIC FEE AMOUNT =	$ 860.00	
Surcharge of **$130.00** for furnishing the oath or declaration later than □ 20 □ 30 months from the earliest claimed priority date (37 CFR 1.492(e)).	$ 00.00	

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total claims	9 - 20 =	0	x **$18.00**	$ 00.00	
Independent claims	1 - 3 =	0	x **$80.00**	$ 00.00	
MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+ **$270.00**	$ 00.00	
TOTAL OF ABOVE CALCULATIONS =				$ 860.00	
□ Applicant claims small entity status. See 37 CFR 1.27. The fees indicated above are reduced by 1/2. +				$ 00.00	
SUBTOTAL =				$ 860.00	
Processing fee of **$130.00** for furnishing the English translation later than □ 20 □ 30 months from the earliest claimed priority date (37 CFR 1.492(f)).				$ 00.00	
TOTAL NATIONAL FEE =				$ 860.00	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00** per property +				$ 00.00	
TOTAL FEES ENCLOSED =				$ 860.00	
				Amount to be refunded:	$
				charged:	$

a. ☒ A check in the amount of $ 860.00 to cover the above fees is enclosed.

b. □ Please charge my Deposit Account No. ____________ in the amount of $ __________ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 13-3083 . A duplicate copy of this sheet is enclosed.

d. □ Fees are to be charged to a credit card. **WARNING:** Information on this form may become public. **Credit card information should not be included on this form.** Provide credit card information and authorization on PTO-2038.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137 (a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

Peter L. MICHAELSON
MICHAELSON & WALLACE
Parkway 109 Office Center
328 Newman Springs Road
P.O. Box 8489
Red Bank, NJ 07701

Peter L Michaelson
SIGNATURE

Peter L. Michaelson
NAME

30.090
REGISTRATION NUMBER

Customer No. 007265

(PTT124TRANS/75:ca)

IN THE UNITED STATES
RECEIVING OFFICE (RO/US)

Applicants: **MULLER, Frank; ROELOFSEN, Gerrit;**
PRINS, Sharon C.L.

International Application No.: **PCT/EP00/02617**

International Filing Date: **23 March 2000**

Serial No.: **09/937,415** Filed: **26 September 2001**

Atty. Doc.: **PTT-124(402562US)** Confirmation No.: **9606**

Title: **METHOD FOR AUTHENTICATION OF A STRING OF INPUT CHARACTERS (as amended)**

COMMISSIONER FOR PATENTS
BOX PCT
Washington, D. C. 20231

S I R:

SECOND PRELIMINARY AMENDMENT

Please amend the above-identified patent application, as follows:

IN THE TITLE-

Delete the title and replace with:

--METHOD FOR AUTHENTICATION OF A STRING OF INPUT CHARACTERS--.

Respectfully submitted,

14 November 2001

Peter L Michaelson

Peter L. MICHAELSON, Attorney
Reg. No. 30,090
Customer No. 007265
(732) 530-6671

MICHAELSON & WALLACE
Counselors at Law
Parkway 109 Office Center
328 Newman Springs Road
P.O. Box 8489
Red Bank, New Jersey 07701

EXPRESS MAIL CERTIFICATION

"Express Mail" mailing label number: **EL632364799US**
Date of deposit: **15 November 2001**

I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Commissioner for Patents, **Box PCT**, Washington, D.C. 20231.

Peter L Michaelson
Signature of person making certification

Peter L. MICHAELSON
Name of person making certification

(PTT124PREAMEND/78:ca)

IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

PATENT APPLICATION

Applicants: **MULLER, Frank; PRINS, Sharon Christie Lesley; ROELOFSEN, Gerrit**

International Application No.: **PCT/EP00/02617**

International Filing Date: **23 March 2000**

Priority Date Claimed: **01 April 1999**

Case: **PTT-124(402562US)**

Title: **METHOD FOR ENCIPHERING A SERIES OF SYMBOLS APPLYING A FUNCTION AND A KEY**

Commissioner for Patents
BOX PCT
Washington, D. C. 20231

S I R:

PRELIMINARY AMENDMENT

Please amend the above-identified patent application which is simultaneously filed herewith, as follows:

IN THE CLAIMS-

To facilitate entry of the following changes, the Applicants have also submitted herewith substitute/clean pages providing all the pending claims, as they now stand.

Delete claims 1-8 and substitute therefore the following claims:

--9. Method for authentication of a string of input characters by means of an enciphering function enabled for enciphering said string of input characters under control of a string of key characters, comprising the steps of:

modifying, by application of a modification function, under control of a string of modification characters, said enciphering function;

enciphering, by application of an enciphering function, under control of said string of key characters, said string of input characters,

CHARACTERIZED in that

said modification function is applied initially, prior to said application of the enciphering function; and

said initially applied modification function modifies the enciphering function under control of modification characters which are derived from said string of input characters.

10. Method according to claim 9, characterized in that said modification characters are also derived from said string of key characters.

11. Method according to claim 9, characterized in that the modification function comprises the replacement of a character of the string of modification characters, by a replacement character obtained by an addition of two or more characters of the string of modification characters modulo the number of possible different characters.

12. Method according to claim 9, characterized in that the modification function comprises the modification of sequence

numbers of two or more of the characters of the string of modification characters.

13. Method according to claim 9, characterized in that, for the modification of the function, there is used as an initial function the function which was used earlier for determining an earlier string of output characters.

14. Method according to claim 9, characterized in that the function is a substitution function.

15. Method according to claim 9, characterized in that the function is a non-invertible function.

16. Method according to claim 9, characterized in that the function comprises a substitution box containing replacement characters for the characters of the string of input characters, and the modification function containing the exchange, depending on the string of modification characters, of two or more characters of the substitute box.

17. Method according to claim 10, characterized in that the modification function comprises the replacement of a character of the string of modification characters, by a replacement character obtained by an addition of two or more characters of the string of modification characters modulo the number of possible different characters. --.

REMARKS

The foregoing amendment is made to conform the claims in the application to that amended in the

International Preliminary Examination Report, to delete multiple dependent claims and to correct minor typographical errors.

Respectfully submitted,

25 September 2001

Peter L. Michaelson, Attorney
Reg. No. 30,090
Customer No. 007265
(732) 530-6671

MICHAELSON & WALLACE
Counselors at Law
Parkway 109 Office Center
328 Newman Springs Road
P.O. Box 8489
Red Bank, New Jersey 07701

*****EXPRESS MAIL CERTIFICATION*****

"Express Mail" mailing label number: **EL632364856US**
Date of deposit: **26 September 2001**

I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Commissioner for Patents, **BOX PCT**, Washington, D.C. 20231.

Signature of person making certification

Peter L. MICHAELSON
Name of person making certification

(PTT124PREAMEND/75:ca)

Method for authentication of a string of input characters

The invention relates to a method according to the preamble of claim 1.

A method of said type is disclosed in EP-A-0399587. With the known method, the function ("algorithm") applied for enciphering consists of a non-linear function formed by a substitution box ("S box") generated as a function of the key. The document provides no further description of the way in which the substitution box is generated. For obtaining good statistical properties of the output of the substitution box with respect to variable import, a string of characters obtained by applying the substitution box are combined with just as long a string of statistically well-distributed characters. The string of characters obtained in this connection may be used for enciphering a string of input characters to be enciphered in an enciphered string of output characters. By applying a key-dependent substitution box instead of a permanent substitution box, the enciphering function is reinforced.

An objection to the known method is that, when there is substantially always used the same key, said reinforcement of the enciphering function in practice is appreciably annihilated. Such may occur, e.g., upon authentication when using a chip card, such as a calling card and a GSM card.

The object of the invention is to exclude the drawbacks of the known method. To this end, the invention provides a method as described in claim 1.

The sender of the enciphered string of output characters and the receiver of said series must both dispose of the same key and the string of input characters used for enciphering, at any rate the portion of the latter series used for modifying the function. As a result, the method is particularly suited for authentication, the receiver of an enciphered string of characters being capable of checking whether a sender having an identity suggested to the receiver has utilised a corresponding key, and in the event of a positive outcome of said check, the identity of the sender is ensured to the receiver.

The string of characters used for modifying the function are particularly variable and are, e.g., a challenge number generated per session, any (different) number, or a variable attribute of the sender, such as a balance kept up to date on a chip card.

If the non-linear function used for enciphering were an invertible function, the receiver of the enciphered string of characters may carry

out said check using the same function, the same key and the received string of characters as an input for the function. The result must be equal to the string of input characters used for enciphering.
Since the receiver may also carry out the check by executing the same operations as the ones carried out by the sender, the series received by the receiver having to be equal to the series generated by the receiver. In such case, it is not required that the function be an invertible function, as a result of which, in the event of the complexity remaining constant, there may be realised a stronger enciphering function which is more resistant against attacks.

The function applied to enciphering preferably is a non-linear function which may be formed by way of a substitution box or a cryptographic function, such as a function in which, depending on the input and the key, specific operations are carried out or not.

It is noted that EP0801477 discloses an encryption method in which an "internal state" is controlling an encryption function which, in each encryption round, modifies the encryption function. According to the present invention, the encryption function is modified only once, in an initial step, while always, after the initial modification, the same encryption function is used in every new encryption round. Contrary to that in the known method the encryption function is modified in every encryption round. Further, in the known method the encryption function is not modified on the basis of the input text. According to the present invetnion the input text forms an essential parameter in modifying the encryption function.

Next, it is noted that US4979832 discloses an enciphering method in which a pseudo-random input string is added to an encryption function. The pseudo-random string used in the encryption function also has to be available in the decryption process. In the known method the encryption function is dynamically (continuously) modified during the encryption processes. This is essential in the method according otherwise the system would be highly insecure. According to the present invention, however, there is only an initial modification of the encryption function, prior to the encryption process itself. Consequently, during the subsequent encryption process the encryption function is not changed any more. The known method is aimed at encryption/decryption. The method according to the invention is specifically designed for authentication and even can in practice not be used for encryption/decryption.

Further properties and advantages of the invention will become clear from the explanation following below of embodiments of the invention in conjunction with the enclosed drawings, in which:

FIG. 1 shows a diagram of a known enciphering function;

FIG. 2 shows a diagram of a first embodiment of the invention;

FIG. 3 shows a flow diagram for the operation of the embodiment according to FIG. 2; and

FIG. 4 shows a different embodiment of the invention.

By way of a block 1, FIG. 1 presents a known enciphering function (or encryption function). The enciphering function utilises one or more functions 2, also presented by blocks. Assuming a string of input characters IN 3 to be enciphered, the enciphering function using a secret key 4 determines an enciphered string of output characters EXIT 5. The known enciphering function DES [= Data Encryption Standard] operates according to said principle, eight non-linear functions being used which are formed by substitution boxes ("S boxes"). The invention is not limited, however, to the DES function; neither is it limited to using non-linear functions and substitution boxes for the functions.

FIG. 2 shows a diagram of an enciphering function 7 based on the enciphering function of FIG. 1 according to the invention. The functions are indicated by reference numeral 8. The functions 8 may be modified by applying an associated reference function 9 based on the string of input characters IN 3 or part thereof. The modification functions 9 need not be equal.

Below, the operation of the enciphering function of FIG. 2 will be explained with reference to the flow diagram of FIG. 3.

A modification function 9 modifies the function 8 based on a string of modification characters initially derived from the string of input characters IN 3 (block 11).Modifying the function 8 takes place in several steps, namely, the steps n=0 to n=Nmax inclusive, Nmax being permitted to be permanent or also depending on, e.g., the series IN 3. That is why, at the start of the modification of the function 8, a step counter is reset (block 12). Subsequently, the function 8 is modified, based on the value of n and the modification series (block 13). Then the number of steps counted is incremented by 1 (block 14).Subsequently, it is checked whether the function 8 has already been modified the maximum number of times (block 15).When this condition is met, the modification of the function 8 is terminated; otherwise the string of modification characters are modified (step 16) and the function 8 is modified once again based on the new value of n and the modified string of modification characters (step

13).In Box I following below, an example is given for the operation of the enciphering function 7 shown in FIG. 2.

TABLE I

Step n	String of modification characters for n>0 x(2):= (x(0) + x(1))mod8			From step n=0, exchange y(nmod8) and y(x(0))								
				i	0	1	2	3	4	5	6	7
	x(0)	x(1)	x(2)	y(i)	3	0	5	7	6	4	1	2
0	5	2	3		4	0	5	7	6	3	1	2
1	2	3	7		4	5	0	7	6	3	1	2
2	3	7	5		4	5	7	0	6	3	1	2
3	7	5	2		4	5	7	2	6	3	1	0
4	5	2	4		4	5	7	2	3	6	1	0
5	2	4	7		4	5	6	2	3	7	1	0
6	4	7	6		4	5	6	2	1	7	3	0
7	7	6	3		4	5	6	2	1	7	3	0
8	6	3	5		1	5	6	2	4	7	3	0
9	3	5	1		1	2	6	5	4	7	3	0

It is assumed that the set of characters comprises eight characters, shown in the Table with the numerals 0 to 7 inclusive. It is further assumed that the function 8 is formed by a substitution box. Said box may be realised by a rewritable memory having eight memory locations containing addresses or sequential numbers 1=0...7. The memory locations each comprise one of the characters, each character figuring only once in the memory locations. In Table I, the content of a memory location having address or sequential number i is indicated by y(i). Initially, the memory locations for i=0...7 contain the characters 3, 0, 5, 7, 6, 4, 1, 2, respectively. Said string of characters form an initial substitution box. A character of a string of characters to be enciphered is considered to be address or sequential number i, and is replaced by the character in the memory location having said address. According to the initial substitution box of Table I, e.g., 0 is therefore replaced by 3, 1 by 0, 2 by 5, ..., 7 by 2.

Before a string of characters to be enciphered are actually enciphered, according to the invention the initial substitution box is modified first. According to the example of Table I, modification takes place in ten steps (step n=0 to n=Nmax inclusive). The modification takes place depending on the characters of the string of characters to be enciphered, at any rate of several characters thereof. In Table I, the characters to be enciphered which are used for the modification of the substitution box are the characters 5, 2 and 3 indicated at step n=0. Said characters are allotted to variables x(0), x(1) and x(2), respectively.

During the first step with n=0, the character y(n), i.e., the character 3 of memory location 0, is exchanged with the character y(x(0)), namely, character 4 of location x(0)=5. In Table I, for clarity's sake, the exchanged characters of the substitution box of eight characters are underlined for each of the ten steps n=0, ...9.

Subsequently, there is calculated an auxiliary variable h, which is equal to:

h=(x(0)+x(1)) modulo (the number of possible characters),

or in the example

h=(x(0)+x(1)) modulo 8.

Subsequently, the characters of the string of modification characters x(0), x(1) and x(2) are replaced as follows (":=" means "becomes", i.e., an allotment).

x(0):=x(1),

x(1):=x(2), and

x(2):=h.

For each step, modifying characters based on the step number and the characters of the string of modification characters are repeated a suitable number of times, in the example of Table I Nmax+1=10 times. At the end of said modification function, the initial substitution box:

3, 0, 5, 7, 6, 4, 1, 2

has been replaced by a final substitution box:

1, 2, 6, 5, 4, 7, 3, 0.

Subsequently, the characters of an input series to be enciphered may, according to the order of the characters in the eventual substitution box, be replaced for providing an output string of enciphered characters. As a result, in the example the string of input characters 5, 2, 3 are replaced by 7, 6, 5, respectively. Said string of output characters are used for possible further steps of the enciphering function.

FIG. 4 shows the diagram of an enciphering function 18 which differs from the enciphering function 5 of FIG. 2 in that the modification function 9 is replaced by a modification function 19. Just as the modification function 9, the modification function 19 depends on a number of characters IN 3 to be enciphered, but in addition on a number of characters of the key 4.

Table II offers an example of the operation of the modification function 19.

TABLE II

Step n	String of modification characters for n>0 x(2):=(x(0) + x(1))mod8					From step n=0, exchange y(nmod8) and y(x(0))								
	x(0)	x(1)	x(2)	x(3)	x(4)	i	0	1	2	3	4	5	6	7
						y(i)	3	0	5	7	6	4	1	2
0	5	2	3	2	4		4	0	5	7	6	3	1	2
1	2	3	2	4	7		4	5	0	7	6	3	1	2
2	3	2	4	7	5		4	5	7	0	6	3	1	2
3	2	4	7	5	5		4	5	0	7	6	3	1	2
4	4	7	5	5	6		4	5	0	7	6	3	1	2
5	7	5	5	6	3		4	5	0	7	6	2	1	3
6	5	5	6	3	5		4	5	0	7	6	1	2	3
7	5	6	3	5	2		4	5	0	7	6	3	2	1
8	6	3	5	2	3		2	5	0	7	6	3	4	1
9	3	5	2	3	1		2	7	0	5	6	3	4	1

Table II differs from Table I only in that the string of modification characters x(0), x(1), x(2) are completed by x(3), x(4). The characters x(·3) and x(4) are derived from the key 4. In the example of Table II, the initial string of modification characters is 5, 2, 3, 2, 4. According to Table II, the eventual substitution box is:

2, 7, 0, 5, 6, 3, 4, 1.

The string of input characters IN 3 having the characters 5, 2, 3 is replaced, according to said eventual substitution box, by the enciphered string of output characters EXIT 20 having the characters 3, 0, 5.

The characters of the initial substitution box may be sorted at random for as long as both the sender of a string of enciphered characters UIT 5 and the receiver of the string of enciphered characters use the same initial substitution box. If it is possible to always meet said condition, the enciphering function may be reinforced by using, as an initial substitution box, a substitution box used during a preceding enciphering process, e.g., the most recently used eventual substitution box. If there is a danger that said condition is not always met, it may be provided that the receiver of the string of enciphered characters 5 recalls several of such preceding substitution boxes and uses an older one thereof if deciphering the series received leads to a negative check result.

Since, both during enciphering a string of characters and during deciphering thereof, the keys used must be equal and knowledge must be available on the string of enciphered characters IN 3, the receiver of the enciphered series may carry out exactly the same operation, i.e., enciphering, as the receiver has carried out, and compare the results to one another. In this event, a non-invertible function may be used for the function which, in the event of constant complexity, makes a stronger enciphering function possible.

The modification functions explained in conjunction with Tables I and II serve only as an example. For modifying the string of modification characters there may be applied, e.g., for each step, more than two and/or a different number of modulo additions, and the characters of the modification series may be rearranged in other ways instead of by way of simple shifting.

CLAIMS

1. Method for authentication of a string of input characters (3) by means of an enciphering function (2, 8) enabled for enciphering said string of input characters under control of a string of key characters (4), comprising the steps of:

- modifying, by application of a modification function, under control of a string of modification characters, said enciphering function;
- enciphering, by application of an enciphering function, under control of said string of key characters (4),said string of input characters,

CHARACTERISED in that

- said modification function (9, 19) is applied initially, prior to said application of the enciphering function and
- said initially applied modification function modifies the enciphering function (8) under control of modification characters which are derived from said string of input characters (3).

2. Method according to claim 1, characterised in that said modification characters are also derived from said string of key characters (4).

3. Method according to claim 1 or 2, characterised in that the modification function (9, 19) comprises the replacement of a character of the string of modification characters, by a replacement character obtained by an addition of two or more characters of the string of modification characters modulo the number of possible different characters.

4. Method according to any preceding claim, characterised in that the modification function (9, 19) comprises the modification of sequence numbers of two or more of the characters of the string of modification characters.

5. Method according to any preceding claim, characterised in that, for the modification of the function, there is used as an initial function the function which was used earlier for determining an earlier string of output characters (5, 20).

6. Method according to any preceding claim, characterised in that the function is a substitution function.

7. Method according to any of the claims 1 to 5 inclusive, characterised in that the function is a non-invertible function.

8. Method according to any of the preceding claims, characterised in that the function comprises a substitution box containing replacement characters for the characters of the string of input characters, and the modification function containing the exchange, depending on the string of modification characters, of two or more characters of the substitution box.

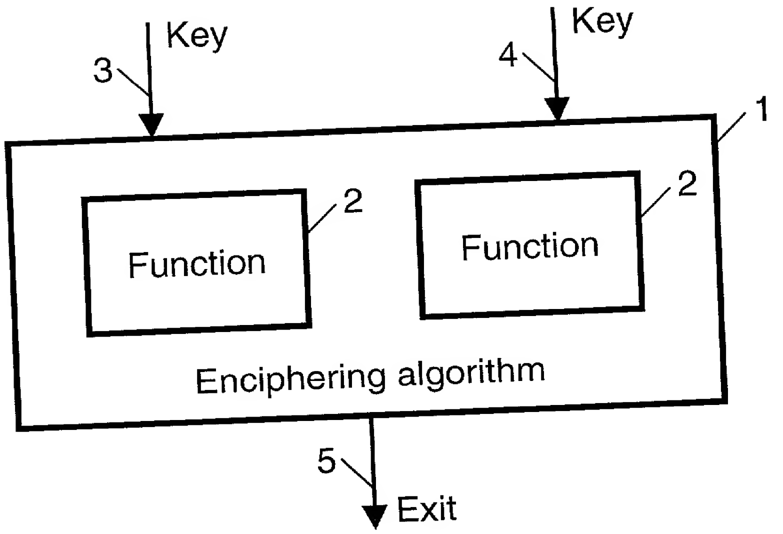
Key
3
Key
4
1
Function
2
Function
2
Enciphering algorithm
5
Exit

FIG 1

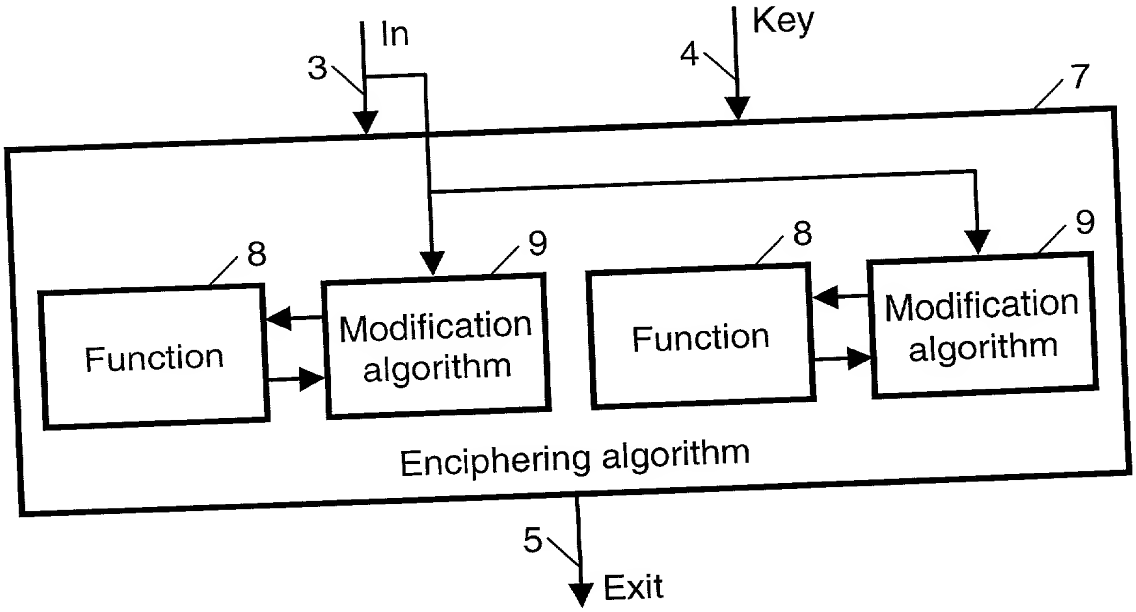
In
3
Key
4
7
8
9
8
9
Function
Modification algorithm
Function
Modification algorithm
Enciphering algorithm
5
Exit

FIG. 2

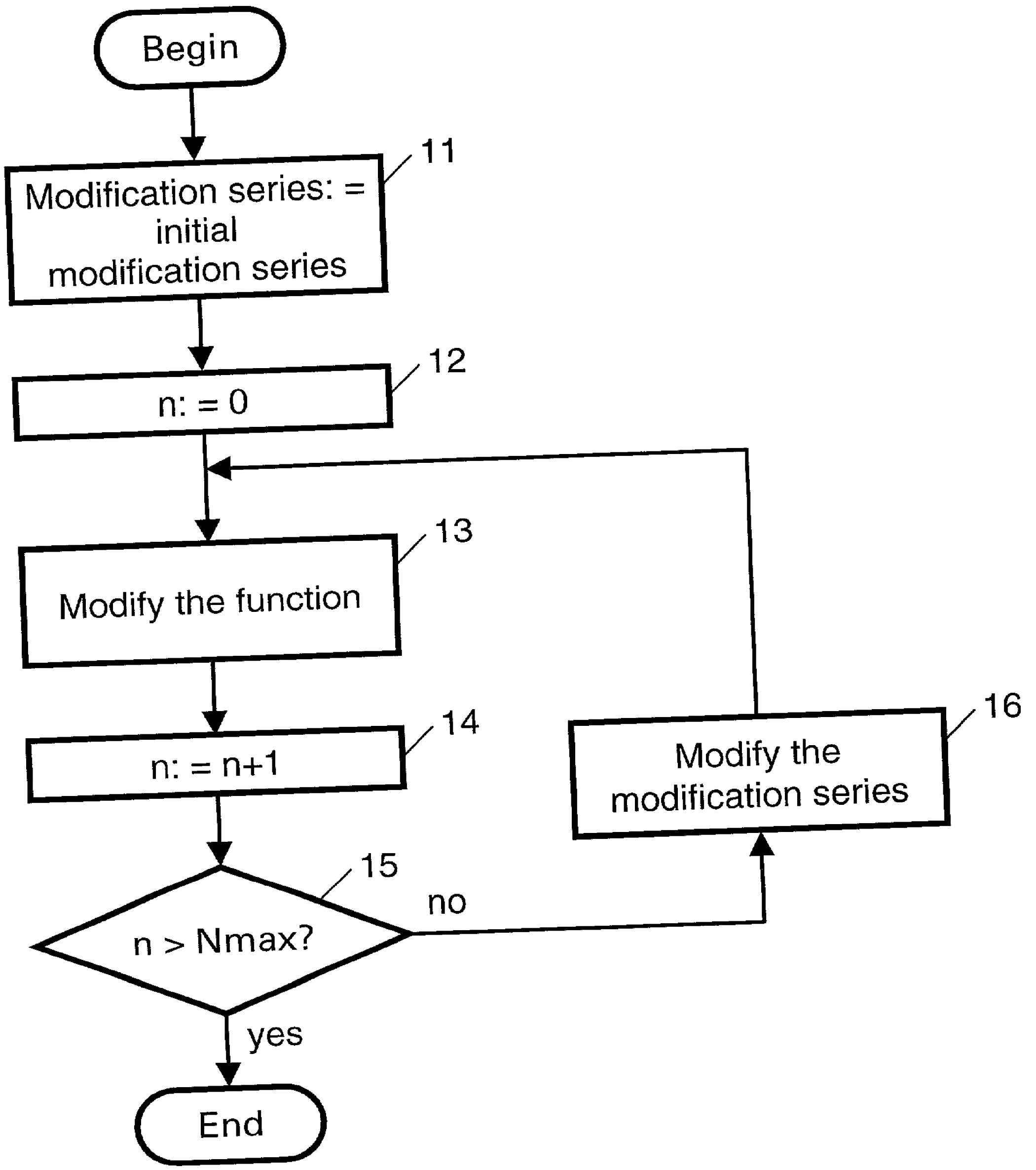
Begin
11
Modification series: = initial modification series
12
n: = 0
13
Modify the function
14
n: = n+1
16
Modify the modification series
15
n > Nmax?
no
yes
End

FIG 3

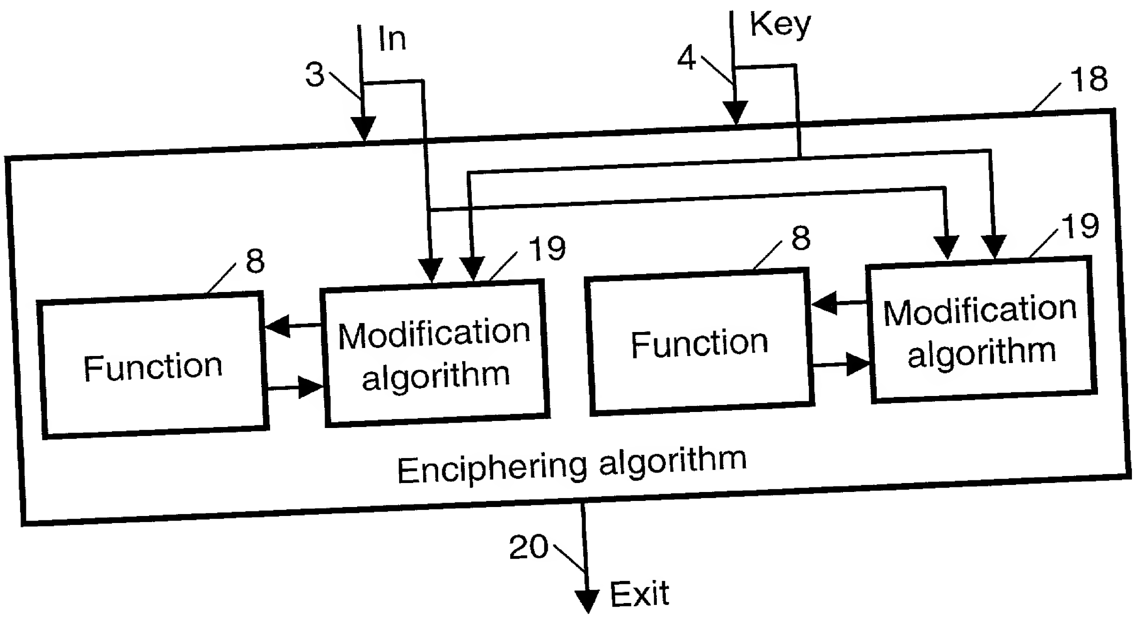
In
3
Key
4
18
8
19
Function
Modification algorithm
8
19
Function
Modification algorithm
Enciphering algorithm
20
Exit

FIG. 4

Atty. Doc. No.: ______________

DECLARATION AND
POWER OF ATTORNEY
(Utility Patent Application)

As a below named inventor, I hereby declare:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below), of the subject matter which is claimed and for which a patent is sought on the invention entitled:

"Method for authentication of a string of input characters."

the specification of which:

__ is attached hereto
__ was filed on ____________ as Application Serial
No. ______________ with amendment(s) filed ________________
__ was filed as PCT international application: PCT/EP00/02617
and was amended under PCT Article 19 on 23 April 2001

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulations section 1.56.

I hereby claim foreign priority benefits under Section 119 of Title 35, United States Code for the above-identified US patent application based on the patent or inventor's certificate identified below and having a filing date before that of the US patent application for which priority is claimed:

Application No	Country	Filing Date	Priority Claimed under 35 USC 119
1011357	NL	February 22, 1999	YES

I hereby claim the benefit under Section 120 and/or Section 119(e) of Title 35 of the United States Code of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by Section 112 of Title 35 of the United States Code, I acknowledge the duty to disclose material information, as defined in Section 1.56 of Title 37 of the Code of Federal Regulations, which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

Application Serial No.	Filing Date	Status Patented	Pending	Abandoned

Power of attorney:

As a named inventor, I hereby appoint:

Peter L. Michaelson (Reg. No. 30,090)
Robert M. Wallace (Reg. No. 29,119)
Jeremiah G. Murray (Reg. No. 20,533)
John T. Peoples (Reg. No. 28,250)
Ronald L. Drumheller (Reg. No. 25,674)
Edward M. Fink (Reg. No. 19,640)
Christopher Balzan (Reg. No. 40,901)
Eric Agaard (Reg. No. 40,478)
Janet M. Skafar (Reg. No. 41,315)
Arthur L. Liberman (Reg.No. 22,698)

as my attorneys to prosecute this application and to transact all business in the United States Patent and Trademark Office in connection therewith.

Direct all correspondence to Customer Number 007265 at the following address:

MICHAELSON & WALLACE
Parkway 109 Office Center
328 Newman Springs Road
P.O. Box 8489
Red Bank, New Jersey 07701.

Direct all telephone calls to: (732) 530-6671.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

First inventor:

100 Full name: MULLER Frank
last first middle

Residence address: Meerkoetlaan 24
Street

2623 NJ DELFT NLX The Netherlands
city, state, zip code country

Post Office address: P.O.Box 95321
post office & box number

2509 CH The Hague The Netherlands
city, state, zip code country

Citizenship: The Netherlands
country

Signature:

Date: 25-9 , 2001

200

Second inventor:

Full name: ROELOFSEN Gerrit
last first middle

Residence address: Rijndijk 60-A
Street

2331 AH LEIDEN NLX The Netherlands
city, state, zip code country

Post Office address: P.O. Box 95321
post office & box number

2509 CH The Hague The Netherlands
city, state, zip code country

Citizenship: The Netherlands
Country

Signature: ______________________

Date: 25-09-2001

300

Third inventor:

Full name: PRINS Sharon Christie Lesley
last first middle

Residence address: Fongersplaats 51
Street

9725 LC GRONINGEN NLX The Netherlands
city, state, zip code country

Post Office address: P.O. Box 95321
post office & box number

2509 CH The Hague The Netherlands
city, state, zip code country

Citizenship: The Netherlands
Country

Signature: ______________________

Date: 19-9-2001